P-2297

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－14871
（P2001－14871A）
(43)公開日　平成13年1月19日(2001.1.19)

(51)Int.Cl.'	識別記号	FI	テーマコード'(参考)
G11C 16/02		G11C 17/00	601P 5B017
G06F 12/14	310	G06F 12/14	310B 5B025
			310F
	320		320D

審査請求　未請求　請求項の数9　ＯＬ　（全８頁）

(21)出願番号　特願平11－183228

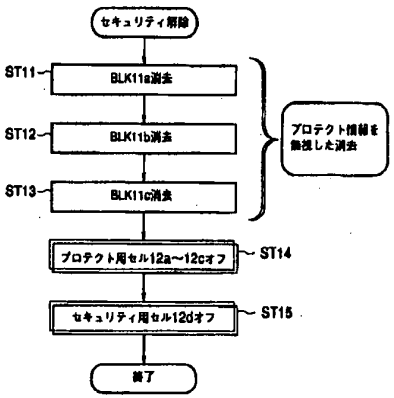
(22)出願日　平成11年6月29日(1999.6.29)

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地
(72)発明者　葛西　央倫
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝マイクロエレクトロニクスセンター内
(72)発明者　西村　望
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝マイクロエレクトロニクスセンター内
(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

最終頁に続く

(54)【発明の名称】　不揮発性半導体記憶装置

(57)【要約】
【課題】本発明は、セキュリティ機能およびプロテクト機能を備えるフラッシュメモリにおいて、セキュリティ機能の解除方法が知られた場合にも、保持データが捏造・漏洩されるのを防止できるようにすることを最も主要な特徴とする。
【解決手段】たとえば、誤書き込みなどによる保持データの破壊を防止するために、プロテクト情報／セキュリティ情報記憶回路内のプロテクト用セルによってプロテクト情報が設定されている状態において、セキュリティ機能の解除が指示されたとする。すると、プロテクト用セルによるプロテクト情報の設定を無視して、各ブロック内のすべての保持データを強制的に消去する。この後、セキュリティ情報の設定を解除することで、たとえ第三者によってセキュリティ機能が解除されたとしても、保持データが外部に漏れるのを防ぐ構成となっている。



【特許請求の範囲】
【請求項１】　保持データを記憶する、書き換え可能型のメモリ手段と、
このメモリ手段における、前記保持データの書き換えを禁止するための書き換え禁止情報を設定することが可能な書き換え禁止手段と、
前記メモリ手段からの、前記保持データの読み出しを禁止するための読み出し禁止情報を設定することが可能な読み出し禁止手段と、
この読み出し禁止手段での前記読み出し禁止情報の設定による読み出し禁止状態を解除する際、前記書き換え禁止手段での前記書き換え禁止情報の設定にかかわらず、前記メモリ手段における前記保持データを消去する消去手段とを具備したことを特徴とする不揮発性半導体記憶装置。
【請求項２】　前記メモリ手段は、記憶エリアが複数のブロックに分割され、各エリアごとに前記書き換え禁止手段による書き換え禁止情報の設定が可能であることを特徴とする請求項１に記載の不揮発性半導体記憶装置。
【請求項３】　前記書き換え禁止手段および前記読み出し禁止手段は、前記メモリ手段内に設けられることを特徴とする請求項１に記載の不揮発性半導体記憶装置。
【請求項４】　前記消去手段は、前記メモリ手段における前記保持データを消去した後に、前記読み出し禁止手段での前記読み出し禁止情報の設定を解除せしめることを特徴とする請求項１に記載の不揮発性半導体記憶装置。
【請求項５】　前記消去手段は、前記メモリ手段における前記保持データを消去した後に、前記読み出し禁止手段での前記読み出し禁止情報の設定、および、前記書き換え禁止手段での前記書き換え禁止情報の設定を、それぞれを解除せしめることを特徴とする請求項１に記載の不揮発性半導体記憶装置。
【請求項６】　保持データを記憶する、書き換え可能型のメモリ手段と、
このメモリ手段における、前記保持データの書き換えを禁止するための書き換え禁止情報を設定することが可能な書き換え禁止手段と、
前記メモリ手段からの、前記保持データの読み出しを禁止するための読み出し禁止情報を設定することが可能な読み出し禁止手段と、
この読み出し禁止手段での前記読み出し禁止情報の設定による読み出し禁止状態を解除する際に、前記書き換え禁止手段での前記書き換え禁止情報の設定による書き換え禁止状態か否かを判断する判断手段と、
この判断手段によって書き換え禁止状態が判断された場合、前記メモリ手段における前記保持データを消去する消去手段と、
この消去手段により、前記メモリ手段における前記保持データが消去された後に、前記読み出し禁止手段での前記読み出し禁止情報の設定を解除する解除手段とを具備したことを特徴とする不揮発性半導体記憶装置。
【請求項７】　前記メモリ手段は、記憶エリアが複数のブロックに分割され、各エリアごとに前記書き換え禁止手段による書き換え禁止情報の設定が可能であることを特徴とする請求項６に記載の不揮発性半導体記憶装置。
【請求項８】　前記書き換え禁止手段および前記読み出し禁止手段は、前記メモリ手段内に設けられることを特徴とする請求項６に記載の不揮発性半導体記憶装置。
【請求項９】　前記解除手段は、さらに、前記メモリ手段における前記保持データが消去された後に、前記書き換え禁止手段での前記書き換え禁止情報の設定を解除せしめることを特徴とする請求項６に記載の不揮発性半導体記憶装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、不揮発性半導体記憶装置に関するもので、特に、セキュリティ機能およびプロテクト機能を備えるフラッシュメモリ（Ｆｌａｓｈ ＥＥＰＲＯＭ (Electrically Erasable Programmable Read Only Memory)）に関するものである。
【０００２】
【従来の技術】周知のように、不揮発性半導体記憶装置としては、ユーザによるオンボード（Ｏｎ－Ｂｏａｒｄ）書き換えが可能なフラッシュメモリがあげられる。このフラッシュメモリには、保持データの捏造・漏洩を防ぐために、保持データの書き換えを禁止する手段（以下、プロテクト機能）、および、保持データの読み出しを禁止する手段（以下、セキュリティ機能）を有するものがある。
【０００３】以下に、従来のフラッシュメモリにおける、プロテクト機能／セキュリティ機能の基本的概念について説明する。
【０００４】図４は、従来のフラッシュメモリにおけるプロテクト機能の基本概念を示すものである。
【０００５】たとえば、フラッシュメモリ本体１０１に対する、保持データの書き換え禁止（プロテクト，オン）状態または書き換え許可（プロテクト，オフ）状態を設定するためのプロテクト情報は、フラッシュメモリ本体１０１とは別の、専用のフラッシュメモリ（Fuse Cell Array）からなるプロテクト情報記憶回路１０２内に記憶されるようになっている。
【０００６】そして、保持データの書き換え／消去時には、たとえば、ステートマシン１０３内の、アンド回路１０３ａによる、コマンドインターフェイス１０４からの信号と上記プロテクト情報記憶回路１０２内のプロテクト情報とのアンド出力にしたがって、書き込み／消去制御回路１０３ｂが制御されるように構成されている。
【０００７】すなわち、上記プロテクト情報記憶回路１０２内のプロテクト情報として、たとえば「１」が記憶

されて，プロテクト，オフが設定されているとすると，上記コマンドインターフェイス１０４からの信号の供給にともなって，上記アンド回路１０３ａからの書き換え信号（アンド出力）が「１（許可）」となる。これにより，ステートマシン１０３による，フラッシュメモリ本体１０１に対する保持データの書き込み／消去が許可される。

【０００８】一方，上記プロテクト情報記憶回路１０２内に「０」が記憶されて，プロテクト，オンが設定されている場合には，上記コマンドインターフェイス１０４からの信号の供給にかかわらず，上記アンド回路１０３ａからの書き換え信号が「０（不可）」となる。これにより，フラッシュメモリ本体１０１に対する保持データの書き込み／消去が禁止される。

【０００９】プロテクト機能とは，こうしたプロテクト情報に応じて，フラッシュメモリ本体１０１に対する，保持データの書き込み／消去の許可／禁止を制御することで，正規ユーザ以外の第三者による保持データの捏造を防止するものである。

【００１０】また，このようなプロテクト機能は，フラッシュメモリ本体の記憶エリア（アドレス領域）が複数のブロックに分割されているフラッシュメモリにおいては，各ブロックごとにプロテクト情報を設定することが可能とされる場合が多い。

【００１１】たとえば，記憶エリアが複数のブロックに分割されているフラッシュメモリ本体の，あるブロック（ＢＬＫ０）内に保持しているデータは書き換え頻度の少ない（または，重要な）プログラムであり，別のブロック（ＢＬＫ１）内に保持しているデータは書き換え頻度の多いデータであるとすると，誤書き込みなどによるデータ破壊がシステムの致命傷となるため，この場合，ブロック（ＢＬＫ０）に対してはプロテクト，オンとし，ブロック（ＢＬＫ１）に対してはプロテクト情報の設定が面倒（Ｗ／Ｅ時間の増加）などの理由から，プロテクト，オフとするといった使用例がある。

【００１２】図５は，従来のフラッシュメモリにおけるセキュリティ機能の基本概念を示すものである。

【００１３】たとえば，フラッシュメモリ本体１０１に対する，保持データの読み出し禁止（セキュリティ，オン）状態または読み出し許可（セキュリティ，オフ）状態を設定するためのセキュリティ情報は，フラッシュメモリ本体１０１とは別の，専用のフラッシュメモリ（Fuse Cell Array）からなるセキュリティ情報記憶回路１０５内に記憶されるようになっている。

【００１４】そして，保持データの読み出し時には，たとえば，データ制御回路１０６内の，アンド回路１０６ａによる，読み出し制御回路１０６ｂからの信号と上記セキュリティ情報記憶回路１０５内のセキュリティ情報とのアンド出力にしたがって，読み出し回路１０７とデータ出力端子Dout との間の設けられたトライステート・バッファ１０８が制御されるように構成されている。

【００１５】すなわち，上記セキュリティ情報記憶回路１０５内のセキュリティ情報として，たとえば「１」が記憶されて，セキュリティ，オフが設定されているとすると，上記読み出し制御回路１０６ｂからの信号の供給にともなって，上記アンド回路１０６ａからの読み出し信号（アンド出力）が「１（許可）」となる。これにより，上記トライステート・バッファ１０８がイネーブル状態となって，上記読み出し回路１０７により上記フラッシュメモリ本体１０１内から読み出された保持データの，上記データ出力端子Dout を介しての読み出しが許可される。

【００１６】一方，上記セキュリティ情報記憶回路１０５内に「０」が記憶されて，セキュリティ，オンが設定されている場合には，上記読み出し制御回路１０６ｂからの信号の供給にかかわらず，上記アンド回路１０６ａからの読み出し信号が「０（不可）」となる。これにより，上記トライステート・バッファ１０８の出力（Ｚ）がＨｉｇｈ－Ｚ（または，固定データ出力）の状態となって，フラッシュメモリ本体１０１からの保持データの読み出しが禁止される。

【００１７】セキュリティ機能とは，こうしたセキュリティ情報に応じて，フラッシュメモリ本体１０１からの，保持データの読み出しの許可／禁止を制御することで，正規ユーザ以外の第三者への保持データの漏洩を防止するものである。

【００１８】また，このようなセキュリティ機能は，フラッシュメモリ本体の記憶エリア（全アドレス領域）に対して，１つのセキュリティ情報を設定することが可能とされる場合が多い。

【００１９】次に，上記したプロテクト情報およびセキュリティ情報の設定方法について，簡単に説明する。

【００２０】図６は，プロテクト情報およびセキュリティ情報の設定方法を説明するために示す概略図である。なお，ここでは，フラッシュメモリ本体の記憶エリアが複数のブロックに分割されている場合を例に説明する。

【００２１】プロテクト情報およびセキュリティ情報を設定する場合，外部トリガ（たとえば，端子情報／コマンド）により，専用のフラッシュメモリ２０１に対する書き換えシーケンスに入る。

【００２２】そして，プロテクト情報を書き換える場合（たとえば，フラッシュメモリ本体の記憶エリアが３つのブロックに分割されているとする）には，アドレス入力端子Ａｄｄより，コマンドインターフェイス２０２および書き込み／消去回路２０３に供給されるブロック情報（アドレス）をもとに，プロテクト情報記憶回路１０２内の，対象のセル１０２ａ，１０２ｂ，１０２ｃに対してオン／オフの設定が行われる。

【００２３】また，セキュリティ情報を書き換える場合には，端子／アドレスなどの情報にしたがって，セキュリティ情報記憶回路１０５を構成するセル１０２ｄの選択が行われた後に，該セル１０２ｄに対するオン／オフの設定が行われる。

【００２４】しかしながら，このような構成のフラッシュメモリにおいては，セキュリティ情報を設定（セキュリティ，オン）することによって，保持データの捏造・漏洩を防止できるものの，セキュリティ機能の解除方法が知られた場合には，第三者に保持データが容易に捏造・漏洩される可能性があるというデメリットがあった。

【００２５】図７は，従来のフラッシュメモリにおける，セキュリティ機能の解除動作にかかる処理の流れを示すものである。

【００２６】たとえば，誤書き込みなどによる保持データの破壊を防止するために，全ブロックＢＬＫについて，プロテクト情報が設定（プロテクト，オン）されている状態において，セキュリティ機能の解除（セキュリティ，オフ）が指示されたとする。

【００２７】すると，セキュリティ情報の設定を解除するためにセキュリティ用セルをオフにするが，この場合，まず，各ブロックＢＬＫのプロテクト情報の設定を順にチェックして，プロテクト，オフのブロックＢＬＫ内の保持データのみ，順次，消去する（ステップＳＴ０１～ＳＴ０３）。

【００２８】しかる後，セキュリティ情報の設定を解除して（ステップＳＴ０４），一連の動作を終了する。

【００２９】すなわち，プロテクト情報が設定されていない場合には，そのブロックＢＬＫ内の保持データの消去を行い，プロテクト情報が設定されている場合には，そのブロックＢＬＫ内の保持データの消去を行わずに，セキュリティ情報の設定が解除される。

【００３０】この場合，保持データが失われないまま，該保持データの読み出しが可能な状態となる。その結果，セキュリティ機能の解除が第三者によって行われた場合には，保持データの内容が第三者に知られることになる。

【００３１】なお，保持データを読み出した後には，再度，当該ブロックＢＬＫ内にデータを書き込む必要があるため，プロテクト用セルをオフにして，プロテクト機能を解除する。

【００３２】そして，当該ブロックＢＬＫ内にデータを書き込んだ後，必要に応じて，プロテクト情報の設定（プロテクト，オン）が行われる。

【００３３】このように，従来は，セキュリティ機能の解除の方法が知られてしまった場合には，第三者による保持データの改ざん（捏造）までもが容易に可能となり，プロテクト機能／セキュリティ機能は全く意味のないものとなるという問題があった。

【００３４】

【発明が解決しようとする課題】上記したように，従来においては，セキュリティ機能の解除方法が知られた場合には，第三者に保持データが容易に捏造・漏洩される可能性があるという問題があった。

【００３５】そこで，この発明は，セキュリティ機能の解除方法が知られた場合にも，保持データが捏造・漏洩されるのを防止でき，保持データの機密性を飛躍的に向上させることが可能な不揮発性半導体記憶装置を提供することを目的としている。

【００３６】

【課題を解決するための手段】上記の目的を達成するために，この発明の不揮発性半導体記憶装置にあっては，保持データを記憶する，書き換え可能型のメモリ手段と，このメモリ手段における，前記保持データの書き換えを禁止するための書き換え禁止情報を設定することが可能な書き換え禁止手段と，前記メモリ手段からの，前記保持データの読み出しを禁止するための読み出し禁止情報を設定することが可能な読み出し禁止手段と，この読み出し禁止手段での前記読み出し禁止情報の設定による読み出し禁止状態を解除する際，前記書き換え禁止手段での前記書き換え禁止情報の設定にかかわらず，前記メモリ手段における前記保持データを消去する消去手段とから構成されている。

【００３７】また，この発明の不揮発性半導体記憶装置にあっては，保持データを記憶する，書き換え可能型のメモリ手段と，このメモリ手段における，前記保持データの書き換えを禁止するための書き換え禁止情報を設定することが可能な書き換え禁止手段と，前記メモリ手段からの，前記保持データの読み出しを禁止するための読み出し禁止情報を設定することが可能な読み出し禁止手段と，この読み出し禁止手段での前記読み出し禁止情報の設定による読み出し禁止状態を解除する際に，前記書き換え禁止手段での前記書き換え禁止情報の設定による書き換え禁止状態か否かを判断する判断手段と，この判断手段によって書き換え禁止状態が判断された場合，前記メモリ手段における前記保持データを消去する消去手段と，この消去手段により，前記メモリ手段における前記保持データが消去された後に，前記読み出し禁止手段での前記読み出し禁止情報の設定を解除する解除手段とから構成されている。

【００３８】この発明の不揮発性半導体記憶装置によれば，書き換え禁止情報の設定にかかわらず，読み出し禁止情報の設定が解除された場合には，メモリ手段における保持データを消去できるようになる。これにより，たとえ第三者が読み出し禁止情報の設定を解除する方法を知ったとしても，保持データが第三者の目に触れるのを避けることが可能となるものである。

【００３９】

【発明の実施の形態】以下，この発明の実施の形態について図面を参照して説明する。

【００４０】（一実施形態）図１は，本発明の一実施形態にかかる不揮発性半導体記憶装置の概略構成を，フラ

ッシュメモリ（Ｆｌａｓｈ ＥＥＰＲＯＭ）を例に示すものである。

【００４１】このフラッシュメモリは、たとえば、フラッシュメモリ本体（書き換え可能型のメモリ手段）１１、プロテクト情報／セキュリティ情報記憶回路１２、コマンドインターフェイス１３、ステートマシン（消去手段）１４、データ制御回路１５、読み出し回路１６、トライステート・バッファ１７、および、電源回路１８を有して構成されている。

【００４２】フラッシュメモリ本体１１は保持データを記憶するためのもので、たとえば、記憶エリア（全アドレス領域）が３つのブロック（ＢＬＫ）１１ａ，１１ｂ，１１ｃに分割されている。

【００４３】プロテクト情報／セキュリティ情報記憶回路１２は、たとえば、上記フラッシュメモリ本体１１とは別の、専用のフラッシュメモリ（Ｆｕｓｅ Ｃｅｌｌ Ａｒｒａｙ）からなり、プロテクト機能（書き換え禁止手段）としての、上記各ブロック１１ａ，１１ｂ，１１ｃにおける保持データの書き換えを禁止するためのプロテクト情報（書き換え禁止情報）をそれぞれ記憶するプロテクト用セル１２ａ，１２ｂ，１２ｃと、セキュリティ機能（読み出し禁止手段）としての、上記全ブロック１１ａ，１１ｂ，１１ｃに対する保持データの読み出しを禁止するためのセキュリティ情報（読み出し禁止情報）を記憶するセキュリティ用セル１２ｄとを有して構成されている。

【００４４】コマンドインターフェイス１３は、たとえば、アウトプットイネーブル信号入力端子（／ＯＥ）、チップイネーブル信号入力端子（／ＣＥ）、ライトイネーブル信号入力端子（／ＷＥ）、ブロック情報（アドレス）入力端子Ａｄｄ、および、データ入力端子（Ｄｉｎ）を介して、それぞれ外部より供給される情報にもとづいて、上記フラッシュメモリ本体１１に対するデータの読み出しか、書き込みか、消去かを判断し、上記ステートマシン１４を制御するものである。

【００４５】ステートマシン１４は、上記コマンドインターフェイス１３の制御のもと、上記プロテクト情報／セキュリティ情報記憶回路１２内に記憶されているプロテクト情報の設定に応じて、上記フラッシュメモリ本体１１に対するデータの書き込み／消去を実行するものである。

【００４６】また、ステートマシン１４は、たとえば図５に示したように、セキュリティ機能の解除（セキュリティ，オフ）が指示された場合には、上記プロテクト情報／セキュリティ情報記憶回路１２内のプロテクト用セル１２ａ～１２ｃをチェックして、プロテクト情報の設定により書き換え禁止（プロテクト，オン）状態かを判断し、書き換え禁止状態であれば、該プロテクト情報の設定を無視して、上記フラッシュメモリ本体１１内の全ブロック１１ａ～１１ｃにおける保持データの消去を行うようになっている（消去手段）。

【００４７】データ制御回路１５は、上記アウトプットイネーブル信号入力端子（／ＯＥ）および上記チップイネーブル信号入力端子（／ＣＥ）からの各情報と、上記プロテクト情報／セキュリティ情報記憶回路１２内に記憶されているセキュリティ情報の設定とに応じて、上記フラッシュメモリ本体１１より読み出された保持データの外部への出力を許可するかを決定し、上記トライステート・バッファ１７を制御するものである。

【００４８】読み出し回路１６は、上記フラッシュメモリ本体１１内の保持データを、ブロック１１ａ～１１ｃごとに読み出して、上記トライステート・バッファ１７に供給するものである。

【００４９】トライステート・バッファ１７は、上記データ制御回路１５の制御にしたがって、上記読み出し回路１６からの保持データをデータ出力端子Ｄｏｕｔに出力するか、または、Ｈｉｇｈ－Ｚの状態となって、その保持データの上記データ出力端子Ｄｏｕｔへの出力を阻止（または、固定データを出力）するものである。

【００５０】電源回路１８は、動作に必要な所望の電位を生成して、各部に供給するものである。

【００５１】次に、上記した構成におけるフラッシュメモリの動作について、簡単に説明する。なお、フラッシュメモリ本体１１に対する保持データの書き込み／消去およびベリファイに関しては、既知の技術（従来のフラッシュメモリと基本的に同じ）であるため、ここでの説明は割愛する。

【００５２】図２は、本発明のフラッシュメモリにおける、セキュリティ機能の解除動作にかかる処理の流れを示すものである。

【００５３】たとえば、誤書き込みなどによる保持データの破壊を防止するために、プロテクト情報／セキュリティ情報記憶回路１２内のプロテクト用セル１２ａ～１２ｃにより、フラッシュメモリ本体１１内の全ブロック１１ａ～１１ｃについて、プロテクト情報が設定（プロテクト，オン）されている状態において、コマンドインターフェイス１３に対してセキュリティ機能の解除（セキュリティ，オフ）が指示されたとする。

【００５４】すると、この指示がステートマシン１４に送られることにより、該ステートマシン１４は、上記プロテクト情報／セキュリティ情報記憶回路１２内の、プロテクト用セル１２ａ～１２ｃのプロテクト情報の設定を無視して、各ブロック１１ａ～１１ｃ内のすべての保持データを強制的に消去する（ステップＳＴ１１～ＳＴ１３）。

【００５５】ここで言う、プロテクト情報の設定を無視した消去とは、本来ならば、プロテクト用セルによって書き換え禁止（プロテクト，オン）状態が設定されていない、書き換え許可（プロテクト，オフ）状態のブロック内で保持されているデータの消去のみを行うべきところ（図３参照）、たとえプロテクト用セルによって書き換え禁止状態が設定されている場合であっても、その設定にかかわらず、当該ブロック内で保持されているデータの消去を可能にすることである。

【００５６】全ブロック１１ａ～１１ｃ内のすべての保持データを消去し終えた後においては、解除手段としての書き込み／消去回路（図６参照）により、プロテクト用セル１２ａ～１２ｃをオフにして、プロテクト情報の設定を解除し、これによりプロテクト機能を解除する（ステップＳＴ１４）。

【００５７】正規のユーザは、新たに所持しているデータをフラッシュメモリ本体１１内に書き込む必要があるため、使い勝手を考えた場合、保持データの消去にともなって、プロテクト用セル１２ａ～１２ｃをオフにしておくのが良い（書き込みを行う際には、プロテクト用セルをオフにする必要があるため）。

【００５８】また、解除手段としての書き込み／消去回路（図６参照）により、セキュリティ用セル１２ｄをオフにして、セキュリティ情報の設定を解除し、これによりセキュリティ機能を解除して（ステップＳＴ１５）、一連の動作を終了する。

【００５９】このように、セキュリティ機能の解除が指示された場合には、プロテクト情報の設定（プロテクト，オン）にかかわらず、フラッシュメモリ本体１１内の保持データをすべて消去した後に、セキュリティ情報の設定を解除（セキュリティ，オフ）するようにしている。

【００６０】したがって、保持データの読み出しが可能な状態となった際には、既に保持データは存在しない。その結果、たとえ何らかの手段によって、何者かにセキュリティ機能の解除方法が知られたとしても、第三者による保持データの解読または改ざんは不可能となる。

【００６１】上記したように、プロテクト情報の設定にかかわらず、セキュリティ情報の設定が解除された場合には、フラッシュメモリ本体における保持データを消去できるようにしている。

【００６２】すなわち、セキュリティ機能の解除が指示された場合には、フラッシュメモリ本体内の保持データをすべて消去した後に、セキュリティ情報の設定を解除するようにしている。これにより、たとえ何らかの手段によって、何者かにセキュリティ機能の解除方法が知られたとしても、保持データが第三者の目に触れるのを避けることが可能となるため、第三者による保持データの解読または改ざんは不可能となる。したがって、正規のユーザ以外に、保持データが捏造・漏洩されるのを防止でき、保持データの機密性を飛躍的に向上させることが可能となるものである。

【００６３】特に、保持データの消去にともなって、プロテクト用セルをオフしてプロテクト情報の設定を解除するようにした場合には、正規ユーザの使い勝手をも向上できる。

【００６４】なお、上記したこの発明の一実施形態においては、プロテクト情報／セキュリティ情報記憶回路を、たとえば、フラッシュメモリ本体とは別の、専用のフラッシュメモリ（Ｆｕｓｅ Ｃｅｌｌ Ａｒｒａｙ）により構成するようにした場合を例に説明したが、これに限らず、たとえばプロテクト情報／セキュリティ情報記憶回路はフラッシュメモリ本体内に設けることも可能である。

【００６５】また、保持データの捏造・漏洩を防止する方法としては、上記した方法以外に、たとえば、プロテクト情報が設定されている保持データが存在する場合には、セキュリティ機能を解除できないようにするなどの方法も考えられる。

【００６６】その他、この発明の要旨を変えない範囲において、種々変形実施可能なことは勿論である。

【００６７】

【発明の効果】以上、詳述したようにこの発明によれば、セキュリティ機能の解除方法が知られた場合にも、保持データが捏造・漏洩されるのを防止でき、保持データの機密性を飛躍的に向上させることが可能な不揮発性半導体記憶装置を提供できる。

【図面の簡単な説明】

【図１】この発明の一実施形態にかかる、フラッシュメモリの概略構成を示すブロック図。

【図２】同じく、フラッシュメモリにおける、セキュリティ機能の解除動作にかかる処理の流れを示すフローチャート。

【図３】同じく、フラッシュメモリにおける、保持データの消去動作にかかる処理の流れを示すフローチャート。

【図４】従来技術とその問題点を説明するために、フラッシュメモリにおけるプロテクト機能の基本的概念を示すブロック図。

【図５】同じく、従来のフラッシュメモリにおけるセキュリティ機能の基本的概念を示すブロック図。

【図６】同じく、プロテクト情報およびセキュリティ情報の設定方法を説明するために、フラッシュメモリの要部の構成を概略的に示すブロック図。

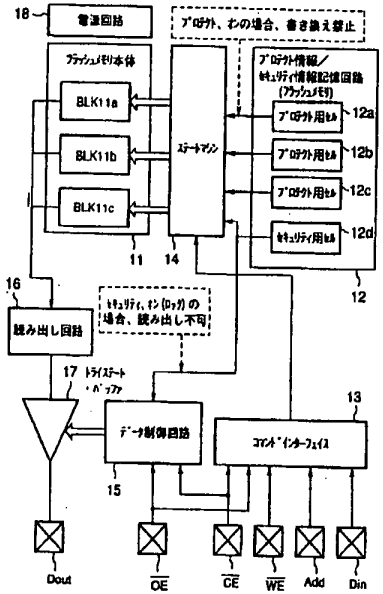
【図７】同じく、従来のフラッシュメモリにおける、セキュリティ機能の解除動作にかかる処理の流れを示すフローチャート。

【符号の説明】

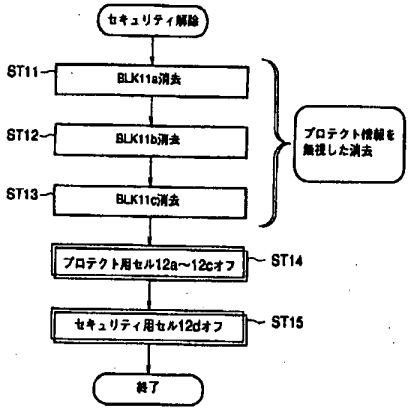
１１…フラッシュメモリ本体
１１ａ，１１ｂ，１１ｃ…ブロック
１２…プロテクト情報／セキュリティ情報記憶回路
１２ａ，１２ｂ，１２ｃ…プロテクト用セル
１２ｄ…セキュリティ用セル
１３…コマンドインターフェイス
１４…ステートマシン
１５…データ制御回路

１６…読み出し回路
１７…トライステート・バッファ
１８…電源回路
／ＯＥ…アウトプットイネーブル信号入力端子
／ＣＥ…チップイネーブル信号入力端子
／ＷＥ…ライトイネーブル信号入力端子
Ａｄｄ…ブロック情報入力端子
Ｄｉｎ…データ入力端子
Ｄｏｕｔ …データ出力端子

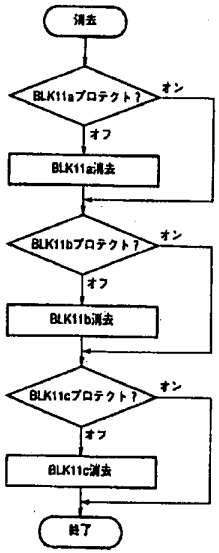
【図１】



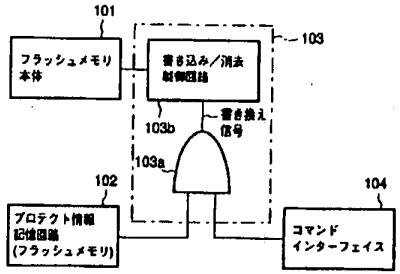
【図２】



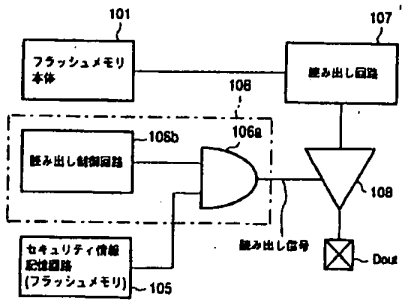
【図３】



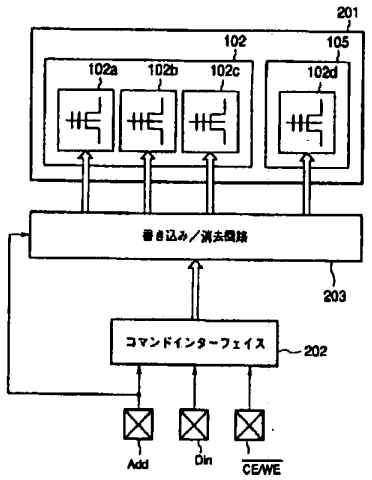
【図４】



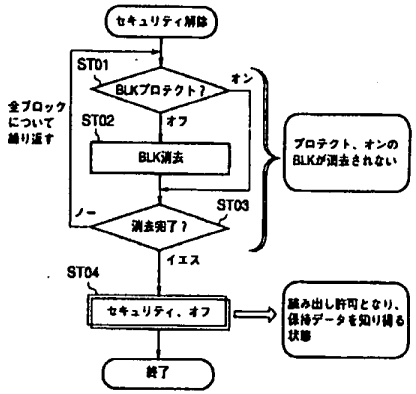
【図５】



【図６】



【図７】



フロントページの続き

Ｆターム(参考) 5B017 AA02 AA03 AA06 BA04 BA08
BA10 BB03 BB05 CA12 CA16
5B025 AA03 AB01 AC01 AD08 AD14
AE10

Nonvolatile semiconductor memory device with security function and protect function

Patent Number: ☐ US6229731
Publication date: 2001-05-08
Inventor(s): KASAI NOZOMI (JP); KASAI TAKAMICHI (JP)
Applicant(s): TOKYO SHIBAURA ELECTRIC CO (US)
Requested Patent: ☐ JP2001014871
Application Number: US20000606146 20000629
Priority Number(s): JP19990183228 19990629
IPC Classification: G11C16/04
EC Classification: G11C16/22
Equivalents:

Abstract

The invention provides a flash memory having a security function and a protect function. When the release of the security function has been instructed, all data stored in each block of a flash memory main body is forcibly erased, ignoring the setting of the protect function. After that, the security function is released, thereby enabling readout of data. This being so, even if a third person releases the security function, leakage of data to the outside can be prevented